Operations Security & Wireless Communications

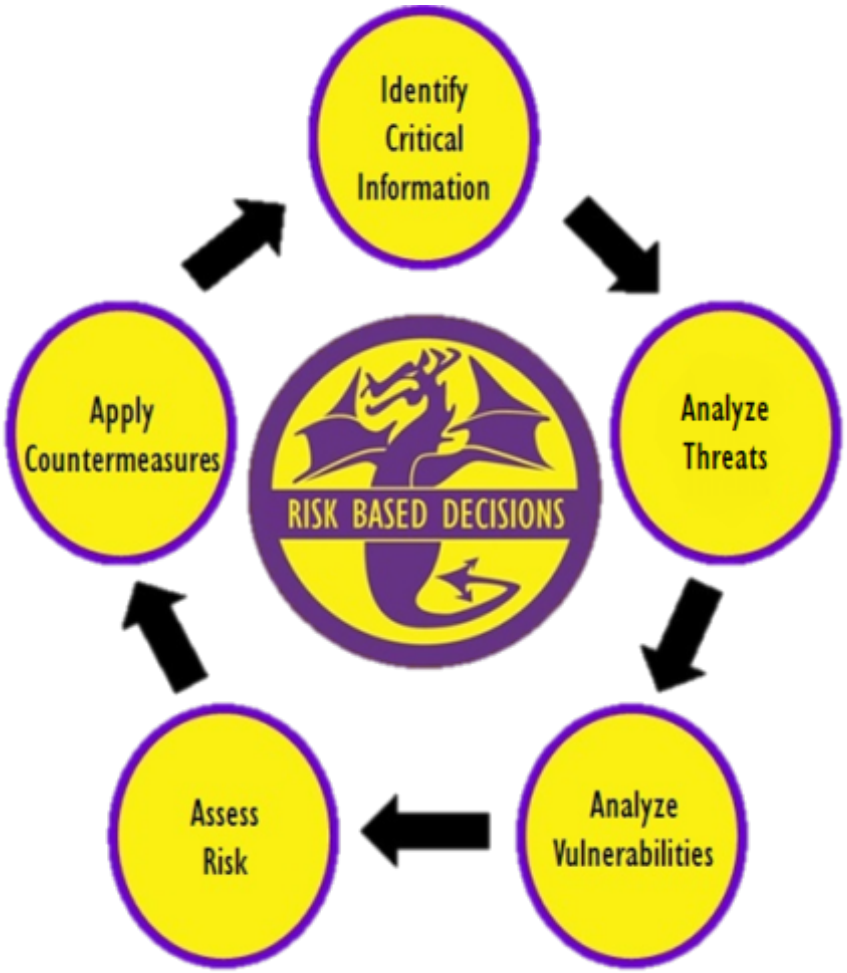
Overall Classification of this Briefing is UNCLASSIFIED

Outline

- OPSEC Overview
- What is wireless
- Use of wireless in the Navy
- Why we can't use wireless
- Wireless threats
- What we can do about it

OPSEC@navy.mil
Http://www.navy.mil/ah_online/OPSEC/index.asp
Facebook.com/NavalOPSEC
@NavalOPSEC
757-417-7100

- **A 5 step process that …**
  - Identifies, controls and protects sensitive, critical unclassified information about a mission, operation or activity
  - Assesses potential threats, vulnerabilities, and risk
  - Utilizes countermeasures to mitigate an adversary's effectiveness against a friendly operation



What is Wireless Communication?

- **Wireless communication is simply:**
  - The transfer of information between two devices that are not connected by an electrical conductor
  - Generally, via a radio frequency signal upon data is transmitted or received

Can We Use Wireless Devices?

- **Yes. But according to DoDD 8100.02…**
  - Wireless devices shall not be used for storing, processing, or transmitting classified information without explicit written approval of the cognizant DAA
  - Cellular/PCS and/or other RF or Infrared (IR) wireless devices shall not be allowed into an area where classified information is discussed or processed without written approval from the DAA in consultation with the Cognizant Security Authority (CSA) Certified TEMPEST Technical Authority (CTTA)
  - Wireless technologies/devices used for storing, processing, and/or transmitting information shall not be operated in areas where classified information is electronically stored, processed, or transmitted unless approved by the DAA
- **Essentially: You cannot operate a wireless device on a DoD network or in a classified area without prior consent of the DAA for the Navy**
- **USFF 131810Z OCT 15**

Why Can't We Use Wireless Devices?

Wireless devices are inherently not secure.

Smartphones

- **Smartphones are some of the most popular and intrusive wireless devices**

More Than Just a Phone

Specs

Processor
- 1 GHz Dual-Core, Dual-Channel RAM processor
- 512 MB RAM

Screen
- 4.3" TFT capactive touchscreen
- Comfortable glasses-free 3D viewing
- 16M color, 800x480 pixels

Android & 3D Apps
- Access to 150,000+ Android Market™ apps
- 3D games from the Gameloft 3D Store™ app
- 3D movies from the mSpot movie™ app

Mobile Hotspot
Share your connection with up to four Wi-Fi-enabled devices

AT&T's 4G Network
The nation's fastest mobile broadband network is getting faster with 4G.*

Memory
- 16 GB total user memory
- Up to 32GB of removeable microSD memory (sold separately)

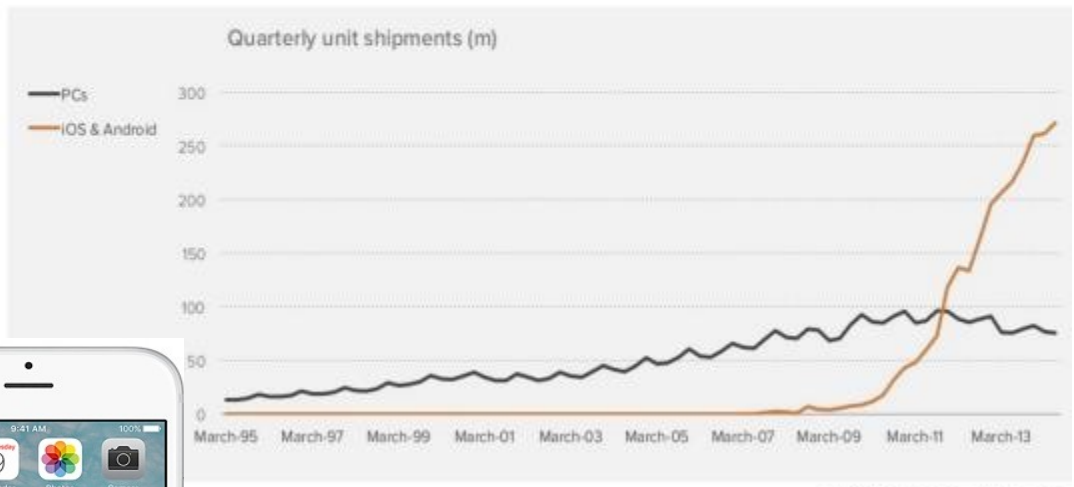
YouTube 3D One-Touch Upload
Post your videos to YouTube 3D right from the sharing menu—exclusively on Thrill

Cameras
- Dual 5MP stereoscopic camera for 3D photo and video capture
- 720p 3D and 1080p 2D High Definition Video Capture
- Front-facing camera for Wi-Fi video chatting**

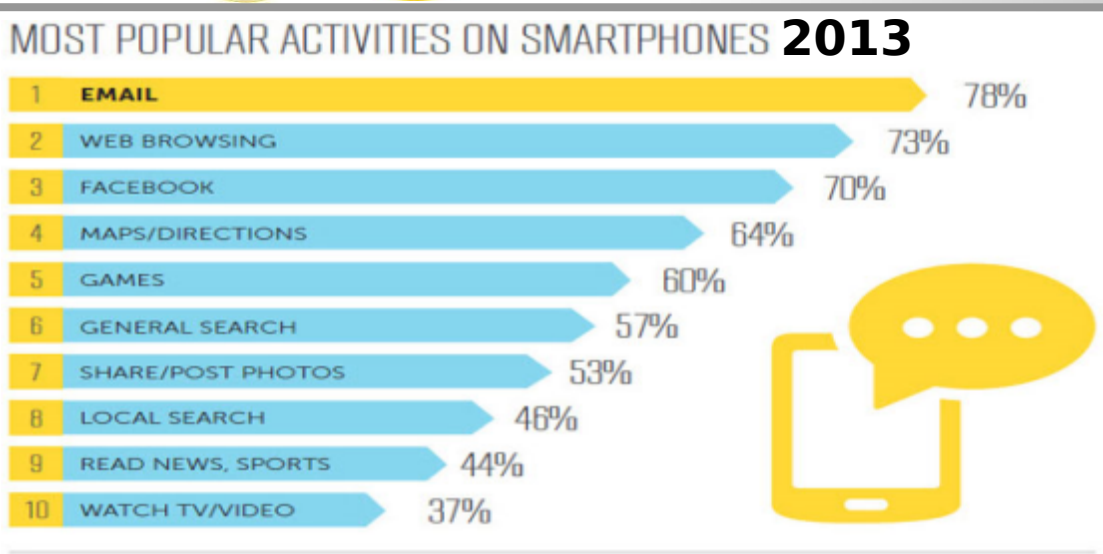
DOWNLOAD SPECS

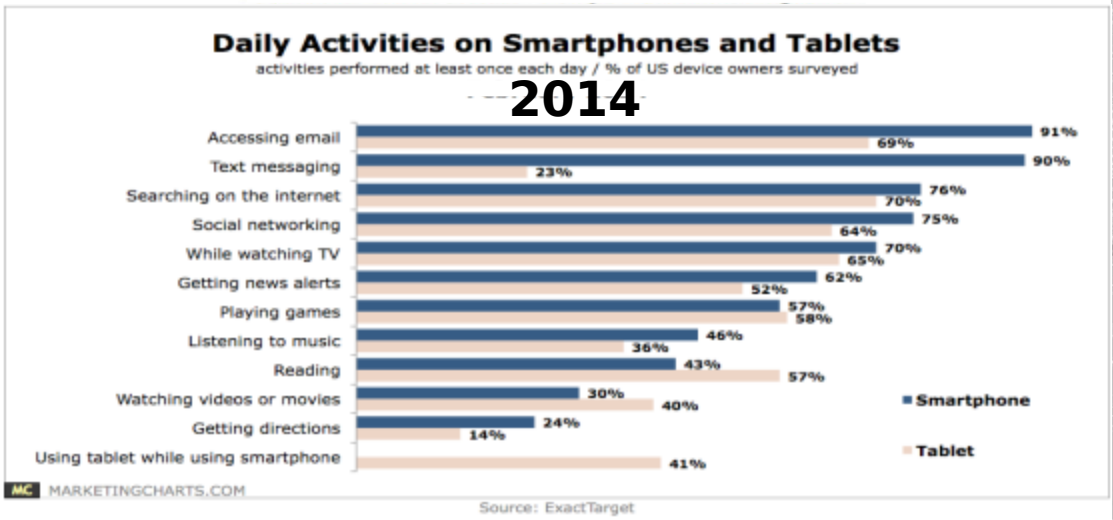
The Future

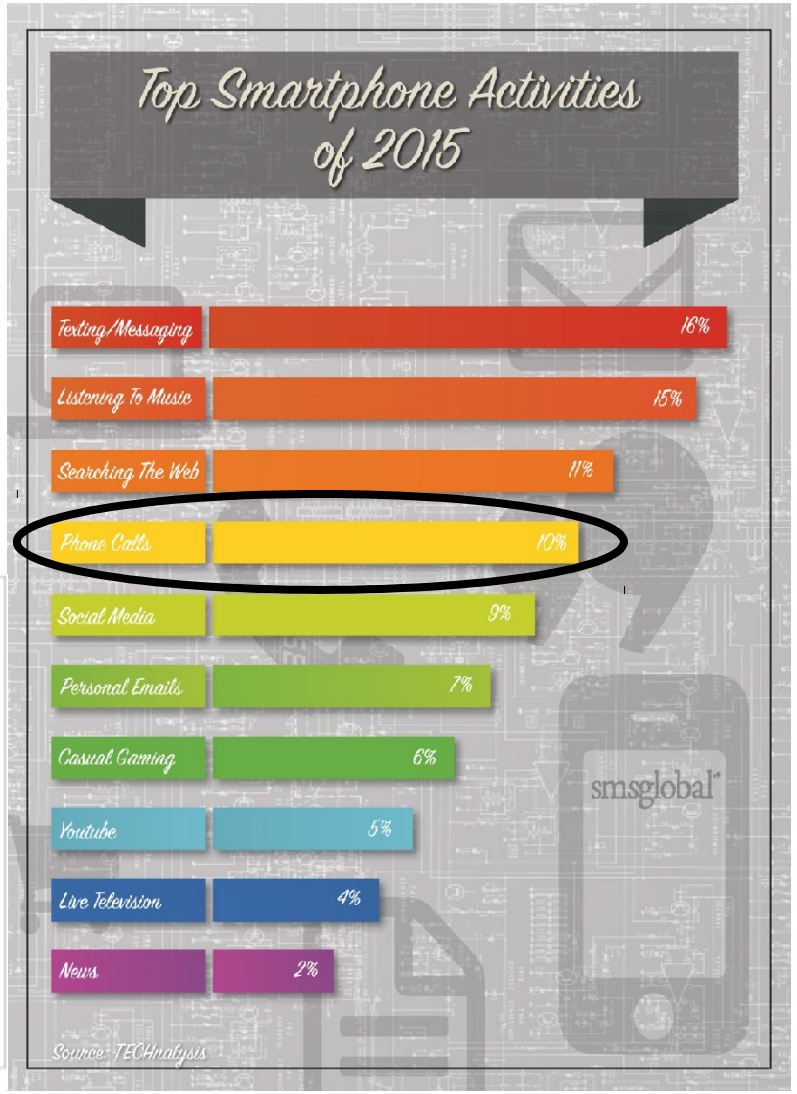
ANDROID SMARTPHONE


The smartphone industry dwarfs PCs
4bn people buying every 2 years instead of 1.6bn buying every 5 years
Quarterly unit shipments (m)
PCs
iOS & Android
300
250
200
150
100
50
0
March-95
March-97
March-99
March-01
March-03
March-05
March-07
March-09
March-11
March-13
Source: Gartner, Apple, Google, a16z

Smartphone Use




Daily Activities on Smartphones and Tablets
activities performed at least once each day / % of US device owners surveyed
2014
Accessing email 91% 69%
Text messaging 90% 23%
Searching on the internet 76% 70%
Social networking 75% 64%
While watching TV 70% 65%
Getting news alerts 62% 52%
Playing games 57% 58%
Listening to music 46% 36%
Reading 43% 57%
Watching videos or movies 30% 40%
Getting directions 24% 14%
Using tablet while using smartphone 41%
Smartphone
Tablet
MARKETINGCHARTS.COM
Source: ExactTarget



But What Are We Really Doing?

- **Smartphones exist for only one reason…**
  - To transmit information from one person to:
    - Another person
    - Many people
    - Everyone
- **What information are we transmitting?**
  - Our conversations
  - Our thoughts and ideas
  - Pictures and videos
  - Metadata
  - Ambient data
  - Unintentional data

Talking

- **Conversation in public**
  - Does everyone around you need to know what you are talking about
  - Does your side of the conversation give away critical information

- **Be aware of your surroundi**
  - Be conscious of the information you are speaking about
  - Who else may be listenir

- **Don’t sell the farm**

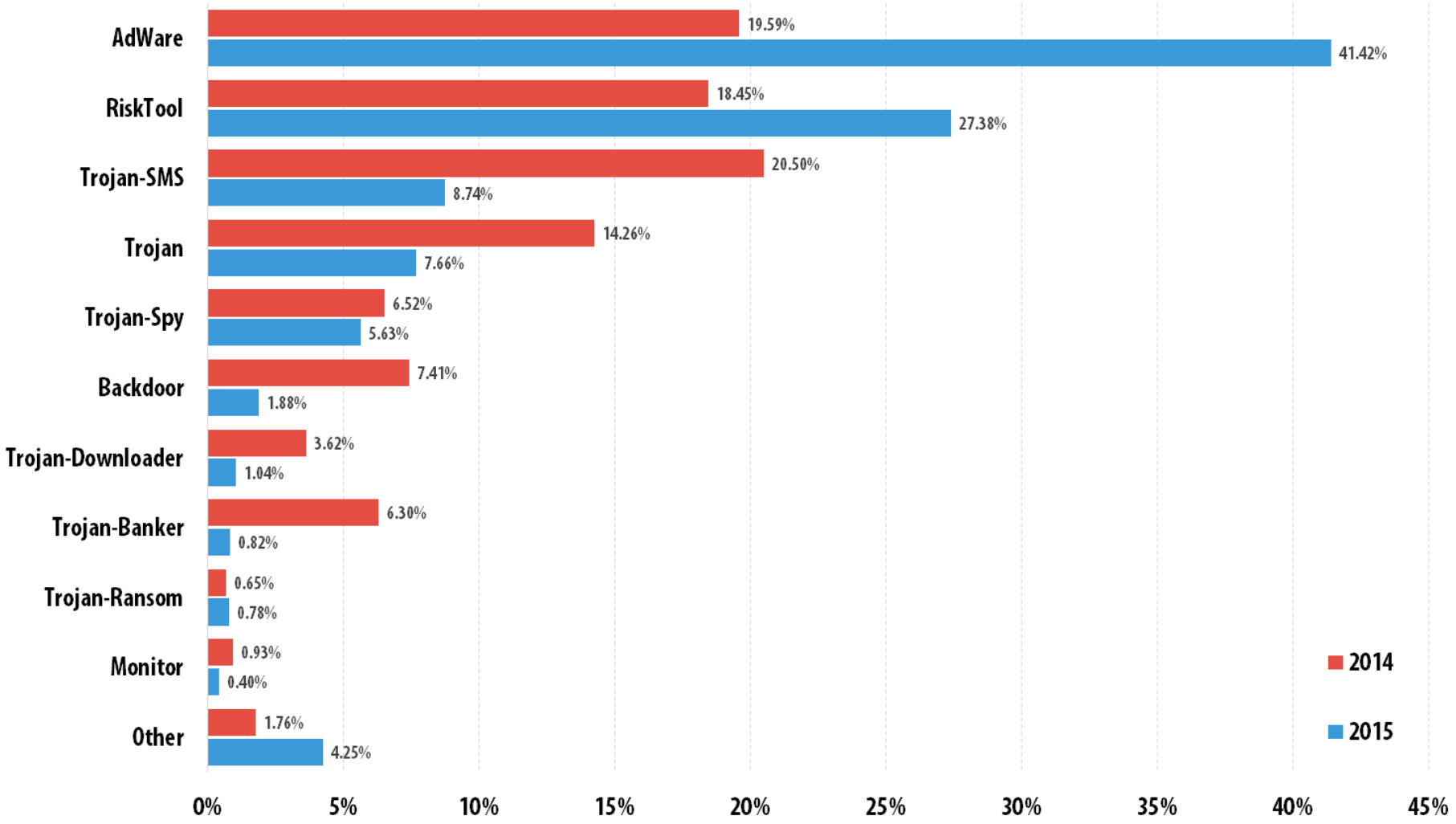
Other Smartphone Capabilities

- GPS and EXIF data
- Microphone
- Bluetooth
- Video Recording
- Accelerometer
- Web browsing
- Near Field Communication
- Radio Frequency Identification

Mobile Trends of 2015

- **Rise in the number of malicious attachments the user is unable to delete**
- **Cybercriminals actively using phishing windows to conceal legitimate apps**
- **Growth in the volume of ransomware**
- **Programs using super-user rights to display aggressive advertising**
- **Increase in the quantity of malware for iOS**
  - 2,961,727 malicious installation packages
  - 884,774 new malicious mobile programs – a threefold increase from the previous year
  - 7,030 mobile banking Trojans

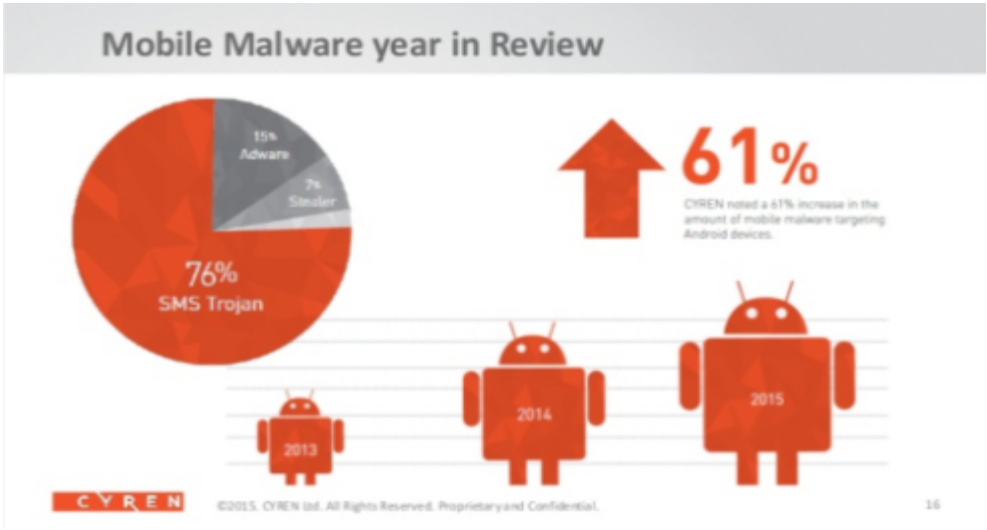
Malware Growth in 2015

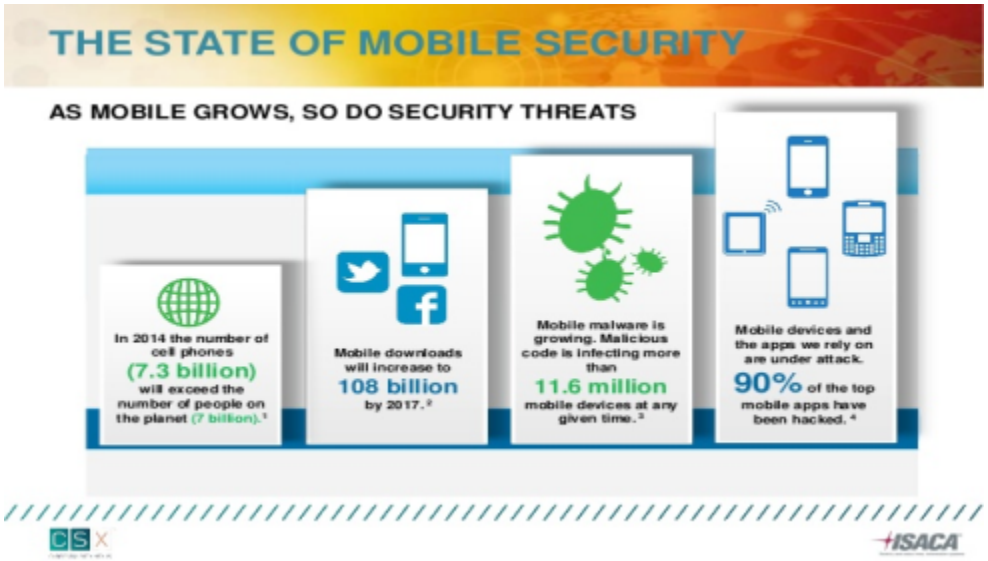


© 2016 AO Kaspersky Lab. All Rights Reserved.

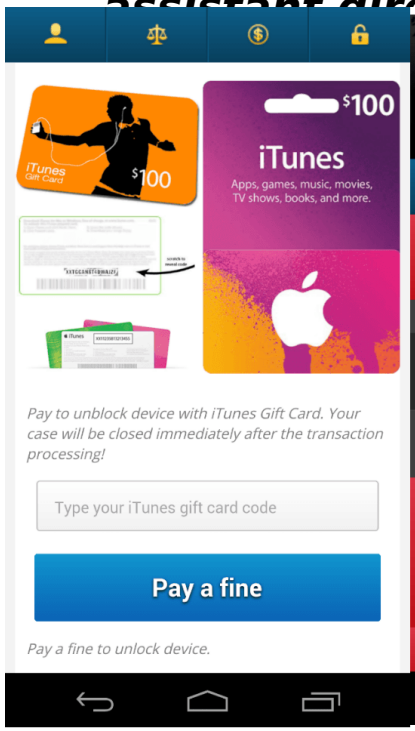
Smartphone Health

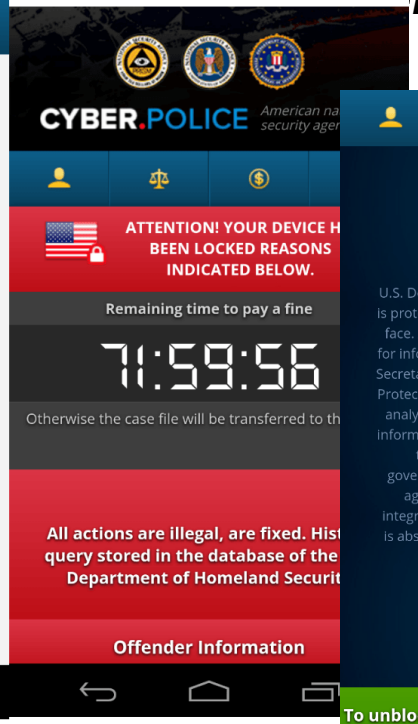
- **Apple iOS Virus May Have Affected Almost 500 apps, 2 Million Users**
  - Forbes.com
- **Only 36 percent of smartphone users have set a 4-digit PIN to lock their phone**
  - Consumer Reports
- **Only 14 percent of the smartphone users have installed an antivirus app**
  - Consumer Reports

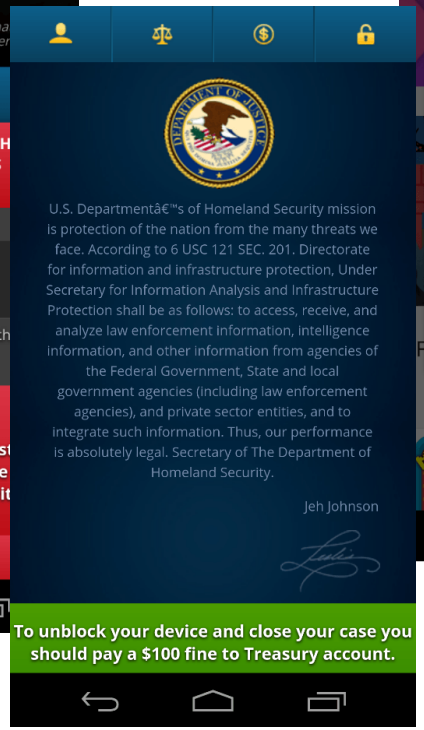


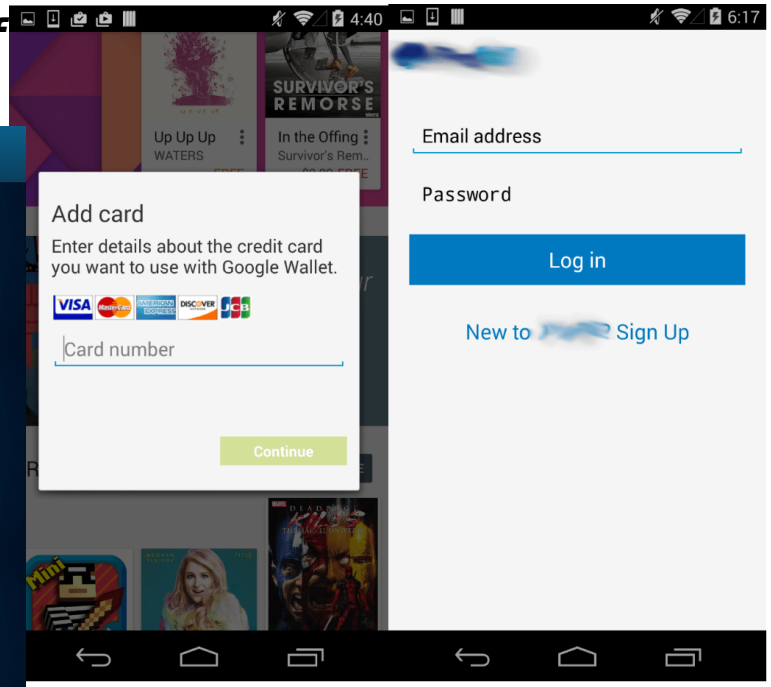

THE STATE OF MOBILE SECURITY
AS MOBILE GROWS, SO DO SECURITY THREATS
In 2014 the number of cell phones (7.3 billion) will exceed the number of people on the planet (7 billion).
Mobile downloads will increase to 108 billion by 2017.
Mobile malware is growing. Malicious code is infecting more than 11.6 million mobile devices at any given time.
Mobile devices and the apps we rely on are under attack. 90% of the top mobile apps have been hacked.
CSX
ISACA

- **"Mobile phones are a huge source of vulnerability. We are definitely seeing an increase in criminal activity."** ***- Gordon Snow, assistant director of the Federal Bureau of***


$100
iTunes
Apps, games, music, movies, TV shows, books, and more.
Pay to unblock device with iTunes Gift Card. Your case will be closed immediately after the transaction processing!
Type your iTunes gift card code
Pay a fine
Pay a fine to unlock device.


CYBER.POLICE
ATTENTION! YOUR DEVICE H
BEEN LOCKED REASONS
INDICATED BELOW.
Remaining time to pay a fine
71:59:56
Otherwise the case file will be transferred to th
All actions are illegal, are fixed. Hist
query stored in the database of the
Department of Homeland Securit
Offender Information

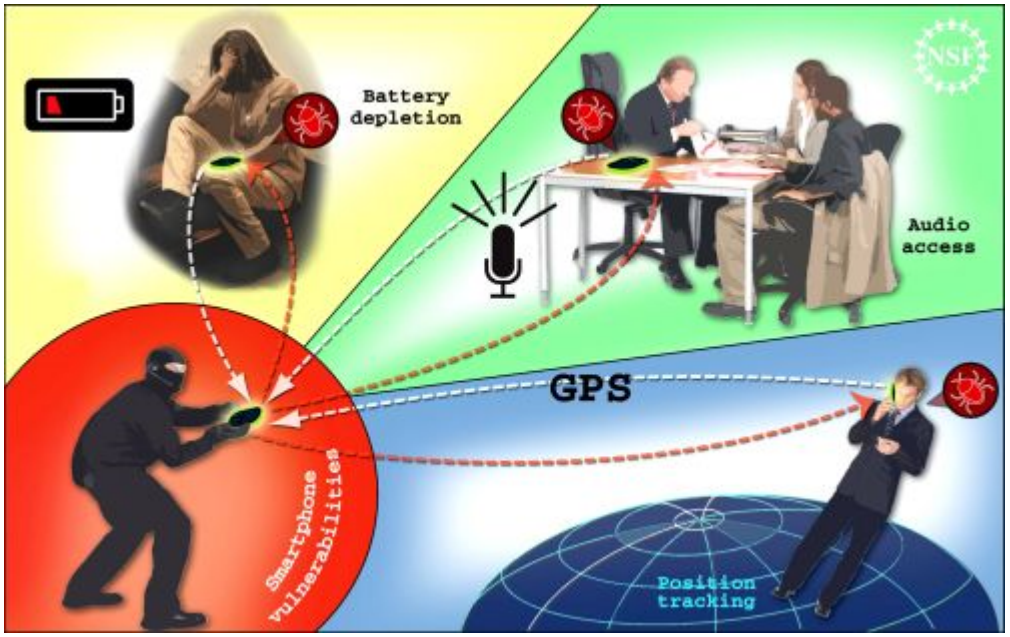

U.S. Departmentâ€™s of Homeland Security mission is protection of the nation from the many threats we face. According to 6 USC 121 SEC. 201. Directorate for information and infrastructure protection, Under Secretary for Information Analysis and Infrastructure Protection shall be as follows: to access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information. Thus, our performance is absolutely legal. Secretary of The Department of Homeland Security.
Jeh Johnson
To unblock your device and close your case you should pay a $100 fine to Treasury account.



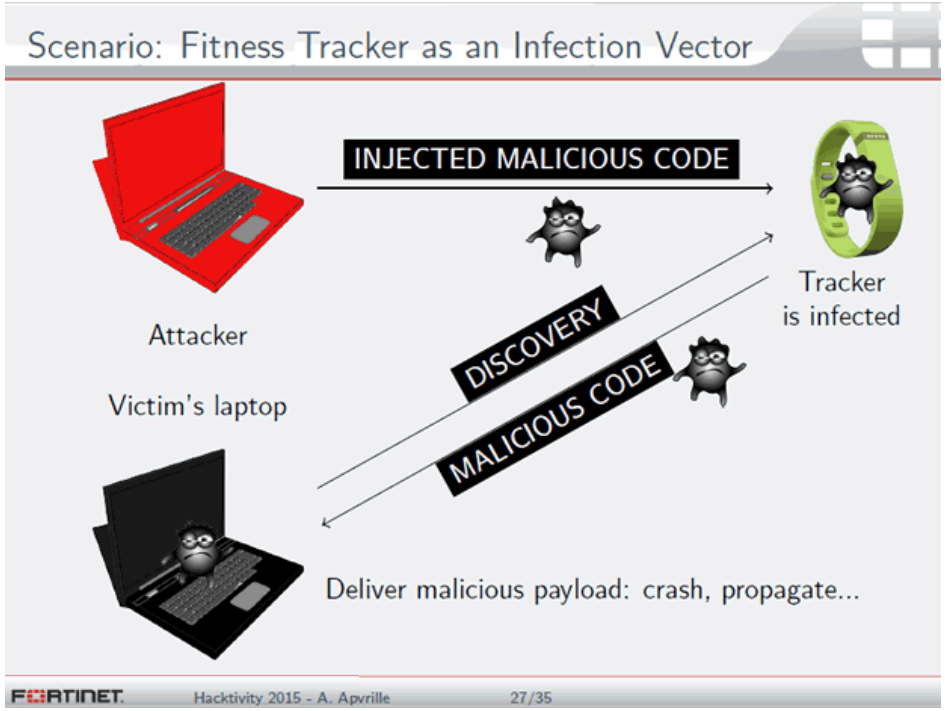
An App for That

- 1.6 million apps available for android
- 1.5 million apps available for iPhone

Before you surrender your life to your smartphone, ensure you research and understand the vulnerabilities that may come with the technology



- **FitBit Wireless vulnerabilities:**
  - Malicious code can be transferred to FitBit by infected servers. FitBit then propagates the virus to other devices via Bluetooth. Virus can then deliver payload to other computers



Cordless Phones

- **Cordless phones are very easy to hack:**
  - Most phones are analog and have no ability to encrypt voice traffic
    - Anyone with a cheap scanner can listen in on your phone call without you knowing
  - Some digital cordless phones have encryp
    - However one only needs an encryption chip i scanner to listen in without your knowledge

WiFi

- **WiFi networks beacon their SSID so wireless devices can locate the network and the network access point**
- **With free and simple to use software, someone could easily hack a WiFi network password that uses WEP, or WPA encryption**
  - If you are not using WPA2 to secure your WiFi network you are vulnerable to attack
- **Wardriving: Driving around to find weakly secured WiFi networks to hack**
- **If you are on the same network as someone else, you are trusting them to have access to ALL of your files**

WiFi Cont.

- **Computers that have Wireless Network Interface Cards are also susceptible to attack:**
  - Attackers can search for and locate Wireless NICs on devices and then remotely connect to those devices
  - This can be done by spoofing the MAC address of a trusted device or simply beaconing the NIC

Understanding the Threat

TABLE I. PERCEIVED UNDERSTANDING OF SECURITY THREATS

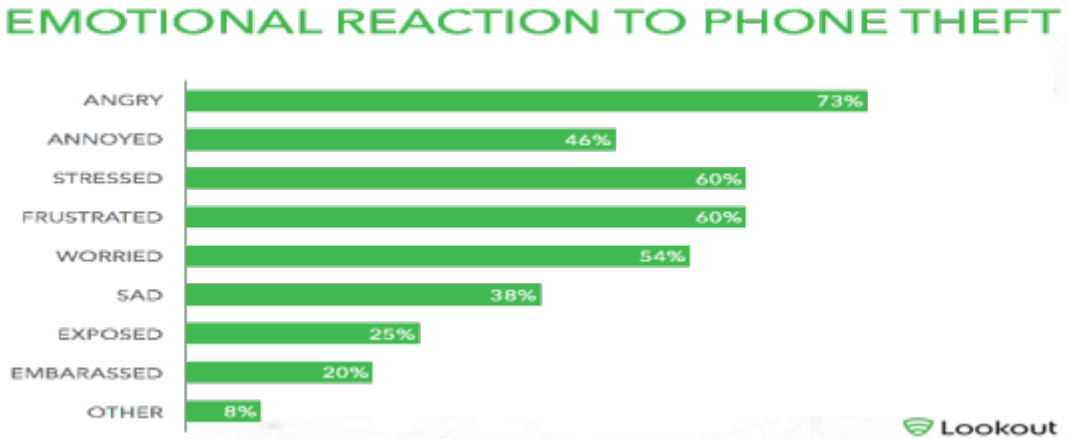
Information Security Terms	You Understand It (%)	You Never Heard Of It (%)
Virus/Worm	92	0
Trojan horse	80	3
Spam	90	0
Social engineering	44	24
Phishing	70	10
Pharming	24	42
Identity theft	81	8
Key loggers	57	22
Phlopping	7	68
Botnets	33	43
Zombies	33	38
Denial of service	56	24
Packet sniffer	47	37
Whooping	10	59
Hacker	95	1
Zero day attacks	29	44
Cracker	56	24

A form of online fraud

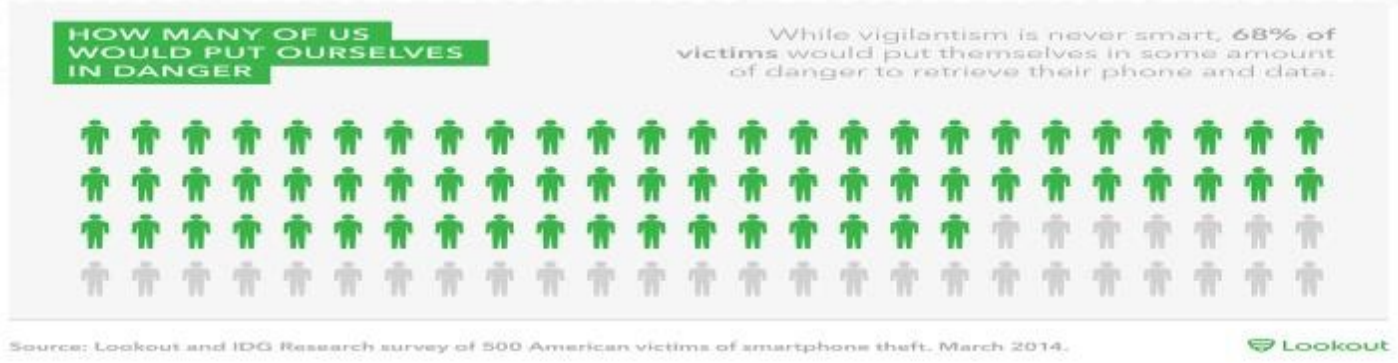
A form of online fraud

CSAN.org

- **How would you feel if your phone was lost or stolen**
- **What would you do to get it back**



WHAT VICTIMS WOULD PAY TO RETRIEVE THEIR STOLEN PHONE
PHONE THEFT VICTIMS WOULD LIKELY PAY
SURPRISINGLY 1 IN THREE
$1,000
TO RETRIEVE THEIR PHOTOS, VIDEOS, APPS & CONTACTS
Lookout


HOW MANY OF US WOULD PUT OURSELVES IN DANGER
While vigilantism is never smart, 68% of victims would put themselves in some amount of danger to retrieve their phone and data.
Source: Lookout and IDG Research survey of 500 American victims of smartphone theft, March 2014.
Lookout

Security Risk

- **What is the biggest security risk when it comes to wireless usage?**

Answer: You……. The user.

Like most people, when it comes to new technology, we want it and we want it now. We usually start using this technology for all the benefits promised without understanding the vulnerabilities or the security features available

- **Top Security apps for Android**

  - CM Security: best malware protection
  - 360 Security - Antivirus: best real-time protection
  - Kaspersky Internet Security: best anti-phishing protection
  - Malwarebytes Anti-Malware: best privacy manager
  - AVL: best interface
  - AVG Antivirus Security: best for protection and anti-theft
  - Norton Security Antivirus: best premium version
  - Avast! Antivirus & Security: most features

» Androidpit.com

From FTC Guardian

- **Draw Something Free** **Grade: D**
  - Access to your phone number, call log, signal information, carrier and more
- **Words With Friends** **Grade: D**
  - Same as Draw Something Free with the added feature of Precise location
- **GO Locker** **Grade: D**
  - Just about every permission available, from your location to reading your text messages
- **My Talking Tom** **Grade: D**
  - Eight targeted ad libraries and, in addition to your phone's identifying information, it sends the advertisers audio from the microphone as well
  - Possible assistance: SnoopWall app - shows which apps are requesting what permissions, selectively granting and retracting access
    - Not an endorsement

Navy Networks

- **In October 2010, CTO 10-084 was released prohibiting the connection of unapproved USB mass storage devices to government networks**
  - This includes connecting a smartphone to a DON computer "just to charge it". Lack of compliance could result in data exfiltration, spillage and the spread of malware

Recommendations

- Never store sensitive data on smart phones
- Enable password protection
- Update device regularly, include anti-virus software
- Do not open suspicious email or click unknown links
- Do not leave phone unattended in public
- Activate lock-out screen
- Enable encryption where possible
- Only purchase apps from legitimate marketplaces
- Turn off GPS & Bluetooth when not in use
- Never “jailbreak” or “root” smartphone
- Understand apps you download/use and what data the app accesses
- Disable Geo-tagging
- Keep phone screen clean
- Data sanitize your device before redistributing

Don’t Be the One

- **Do not be the one who introduces a vulnerability into our DoD networks**
  - Our adversaries are constantly probing our network for weaknesses in order to:
    - Collect critical or classified information
    - Interrupt our ability to communicate
    - Attack our critical infrastructure
    - Decrease our capabilities
    - Decrease our mission effectiveness
- **If you do not understand the risk you cannot assume it**
- **Be a good steward of technology and information**

Summary

- OPSEC Overview
- What is wireless
- Use of wireless in the Navy
- Why we can't use wireless
- Wireless threats
- What we can do about it

Questions

JEB – Little Creek (Bldg 1126)

2555 Amphibious Drive

Virginia Beach, VA 23459-3225

OPSEC@Navy.mil

757-417-7100

Naval OPSEC App

Collaboration at Sea

www.navy.mil/ah_online/OPSEC/index.asp
www.navy.mil/local/OPSEC

Facebook.com/NavalOPSEC

@NavalOPSEC

Youtube.com/USNOPSEC